PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-305558
(43)Date of publication of application : 22.11.1996

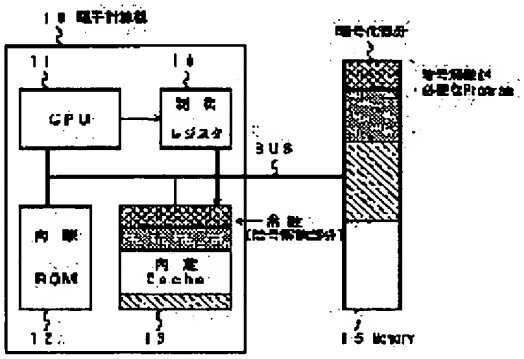
(51)Int.CI. G06F 9/06
G06F 12/14
G09C 1/00
// H04L 9/00
H04L 9/10
H04L 9/12

(21)Application number : 07-104048
(22)Date of filing : 27.04.1995

(71)Applicant : CASIO COMPUT CO LTD
(72)Inventor : HIROYA TAKAYUKI

(54) CIPHERING PROGRAM ARITHMETIC UNIT

(57)Abstract:
PURPOSE: To prevent a ciphered program from being copied and in use in the ciphering program arithmetic unit mounted on an information terminal equipment or the like having a function decoding the ciphered program and executing it.
CONSTITUTION: An electronic computer 10 receives a ciphered part of a ciphered program loaded to an external memory 15, decodes the part according to a ciphering decoding program stored in advance in a built-in ROM 12 unable to be read to an external device and allows a built-in cache memory 13 to store the decoded program. Thus, an inhibit flag of a cache function is set to a control register 14 corresponding to a storage area of the decoded program stored in the built-in cache memory 13 to inhibit the decoded program from being read at an external bus and a CPU 11 executes a combination of the decoded program and the program being non-ciphered parts stored in the external memory 15.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－305558

(43)公開日　平成８年(1996)11月22日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	9/06	５５０		Ｇ０６Ｆ	9/06	５５０Ａ
	12/14	３２０			12/14	３２０Ｂ
Ｇ０９Ｃ	1/00	３１０	7259－5Ｊ	Ｇ０９Ｃ	1/00	３１０
// Ｈ０４Ｌ	9/00			Ｈ０４Ｌ	9/00	Ｚ
	9/10					

審査請求　未請求　請求項の数４　ＯＬ　（全 ７ 頁）　最終頁に続く

(21)出願番号　特願平7－104048

(22)出願日　平成７年(1995)４月27日

(71)出願人　000001443
カシオ計算機株式会社
東京都新宿区西新宿２丁目６番１号

(72)発明者　廣谷　孝幸
東京都羽村市栄町３丁目２番１号　カシオ計算機株式会社羽村技術センター内

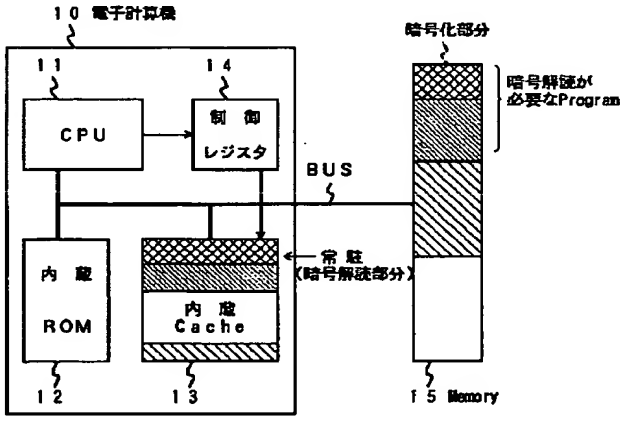
(74)代理人　弁理士　鈴江　武彦

(54)【発明の名称】　暗号化プログラム演算装置

(57)【要約】

【目的】暗号化プログラムを解読して実行する機能を有する情報端末機器等に搭載される暗号化プログラム演算装置において、暗号プログラムがコピーされて利用されるのを防止すること。

【構成】外部メモリ１５にロードされた暗号化プログラムの暗号部分を電子計算機１０に取込んで、外部バスに読出し不可能な内蔵ＲＯＭ１２に予め記憶されている暗号解読プログラム従って解読し、内蔵キャッシュメモリ１３に記憶させると共に、この内蔵キャッシュメモリ１３の前記解読されたプログラムの記憶領域に対応させて、制御レジスタ１４にキャッシュ機能の禁止フラグをセットすることで該解読されたプログラムの外部バスへの読出しも禁止し、この解読後プログラムと前記外部メモリ１５に記憶されている非暗号化部分のプログラムと組合されてＣＰＵ１１により実行される。



1

【特許請求の範囲】
【請求項１】　少なくとも暗号解読プログラムを記憶している第１のメモリと、
この第１のメモリに記憶された暗号解読プログラムにより解読された暗号プログラムを記憶する第２のメモリと、
この第２のメモリに記憶された解読された暗号プログラムの外部への読出しを禁止する読出し禁止手段とを具備したことを特徴とする暗号化プログラム演算装置。
【請求項２】　さらに、前記暗号プログラムの実行モードを記憶する制御レジスタを備え、
この制御レジスタの内容に従って前記第２のメモリに記憶された解読された暗号プログラムの外部への読出しを禁止することを特徴とする請求項１記載の暗号化プログラム演算装置。
【請求項３】　前記暗号解読プログラムにより解読された暗号プログラムを第２のメモリに記憶させる際に、読出し禁止フラグを付けて外部への読出しを禁止することを特徴とする請求項１記載の暗号化プログラム演算装置。
【請求項４】　前記第２のメモリはキャッシュメモリであり、暗号プログラムの実行時は、解読された暗号プログラムの記憶領域の追出し，書込みを禁止することを特徴とする請求項２又は請求項３何れか１項記載の暗号化プログラム演算装置。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、暗号化プログラムを解読して実行する機能を有する情報端末機器等に搭載される暗号化プログラム演算装置に関する。
【０００２】
【従来の技術】近年、コンピュータの急速な普及に伴なって、そのソフトウエアも様々な種類のものが考えられ、汎用ソフトウエアとしてコンピュータの機種に関係なく利用できようになっている。
【０００３】その反面、ソフトウエアの違法なコピーも増加しており、早急にコピー防止の対策を施す必要がある。そこで、ソフトウエアのコピー防止対策の１つとして、ソフトウエアを暗号化し、その実行が許可されたユーザだけが解読プログラムを用いて暗号を解読して利用できるようにしたコピー防止方法が考えられている。
【０００４】ここで、従来の暗号化手法は、ソフトウエアによる変換形態を利用したものが主なものであり、その変換アルゴリズムが複雑であればある程、解読が困難であるのは当然であるが、実際にその暗号化アルゴリズムを作成するのは非常に困難な作業である。
【０００５】
【発明が解決しようとする課題】しかしながら、従来は、暗号解読用のプログラム自体がコピーされて解読されてしまったり、解読された後の暗号プログラムがコピーされて利用される等の問題が生じていた。

2

【０００６】本発明は、前記のような問題に鑑みなされたもので、暗号プログラムがコピーされて利用されるのを防止することが可能になる暗号化プログラム演算装置を提供することを目的とする。
【０００７】
【課題を解決するための手段】すなわち、本発明の請求項１に係わる暗号化プログラム演算装置は、少なくとも暗号解読プログラムを記憶している第１のメモリと、この第１のメモリに記憶された暗号解読プログラムにより解読された暗号プログラムを記憶する第２のメモリと、この第２のメモリに記憶された解読された暗号プログラムの外部への読出しを禁止する読出し禁止手段とを具備したことを特徴とする。
【０００８】また、本発明の請求項２に係わる暗号化プログラム演算装置は、前記請求項１に係わる暗号化プログラム演算装置にあって、さらに、その暗号プログラムの実行モードを記憶する制御レジスタを備え、この制御レジスタの内容に従って前記第２のメモリに記憶された解読された暗号プログラムの外部への読出しを禁止することを特徴とする。
【０００９】また、本発明の請求項３に係わる暗号化プログラム演算装置は、前記請求項１に係わる暗号化プログラム演算装置にあって、その暗号解読プログラムにより解読された暗号プログラムを第２のメモリに記憶させる際に、読出し禁止フラグを付けて外部への読出しを禁止することを特徴とする。
【００１０】また、本発明の請求項４に係わる暗号化プログラム演算装置は、前記請求項２又は請求項３何れか１項に係わる暗号化プログラム演算装置にあって、その第２のメモリはキャッシュメモリであり、暗号プログラムの実行時は、解読された暗号プログラムの記憶領域の追出し，書込みを禁止することを特徴とする。
【００１１】
【作用】つまり、前記請求項１に係わる暗号化プログラム演算装置では、第１のメモリに記憶された暗号解読プログラムにより解読された暗号プログラムが第２のメモリに記憶され、この第２のメモリに記憶された解読された暗号プログラムの外部への読出しが禁止されることになる。
【００１２】また、前記請求項２係わる暗号化プログラム演算装置では、請求項１に係わる暗号化プログラム演算装置にあって、暗号プログラムの実行モードを記憶する制御レジスタの内容に従って第２のメモリに記憶された解読された暗号プログラムの外部への読出しが禁止されることになる。
【００１３】また、前記請求項３に係わる暗号化プログラム演算装置では、請求項１に係わる暗号化プログラム演算装置にあって、暗号解読プログラムにより解読された暗号プログラムが第２のメモリに記憶される際には、

読出し禁止フラグが付けられて外部への読出しが禁止されることになる。

【００１４】また、前記請求項４に係わる暗号化プログラム演算装置は、請求項２又は請求項３何れか１項に係わる暗号化プログラム演算装置にあって、第２のメモリがキャッシュメモリとされ、暗号プログラムの実行時には、解読された暗号プログラムの記憶領域の追出し，書込みが禁止されることになる。

【００１５】

【実施例】以下図面により本発明の実施例について説明する。図１は本発明の第１実施例に係わる暗号化プログラム演算装置を搭載した電子計算機１０の構成を示すブロック図である。

【００１６】この電子計算機１０は、ＣＰＵ１１を備えている。前記ＣＰＵ１１は、内蔵ＲＯＭ１２に予め記憶されているプログラムに従って回路各部の動作制御を実行するもので、このＣＰＵ１１には、データ及び制御バスを介して前記内蔵ＲＯＭ１２の他、内蔵キャッシュメモリ１３が接続される。

【００１７】前記内蔵キャッシュメモリ１３は、その記憶領域を選択的に指示する制御レジスタ１４のセット“１”／リセット“０”によって、当該選択領域におけるキャッシュ機能（データの追出し，書込み機能）の禁止／禁止解除が制御される構成とする。

【００１８】また、前記ＣＰＵ１１は、外部メモリ１５に記憶されているプログラムの読込みを行なった場合には、その読込んだプログラムに従って制御動作を実行する。ここで、前記内蔵ＲＯＭ１２には、予め暗号解読プログラムが記憶され、また、この内蔵ＲＯＭ１２の記憶内容は、外部バスには読出しできない構成とする。

【００１９】なお、前記外部メモリ１５に記憶されるプログラムデータは、例えば公共の有線放送や無線放送、あるいはメモリカード等の利用により得られるデータであってもよい。

【００２０】そして、前記外部メモリ１５から読込まれたプログラムデータが、暗号解読の不要な通常のプログラムデータである場合には、ＣＰＵ１１は内蔵キャッシュメモリ１３の全ての領域についてキャッシュ機能を通常に使用してその読込みプログラムデータにそのまま従った制御動作を実行する。

【００２１】次に、前記第１実施例の構成による暗号化プログラム演算装置を搭載した電子計算機１０における暗号化プログラムの実行動作について説明する。図２は前記第１実施例に係わる暗号化プログラム演算装置を搭載した電子計算機１０における暗号化プログラムの実行処理を示すフローチャートである。

【００２２】すなわち、暗号解読が必要な暗号化プログラムが外部メモリ１５にロードされると、この暗号化プログラムは電子計算機１０に取込まれその暗号部分の解読が開始される（ステップＳ１，Ｓ２）。

【００２３】前記暗号化プログラムは、そのプログラム全体の一部あるいは全てがコマンド，データの区別なく暗号化されており、ヘッダ等において暗号化プログラムであることの情報が付加されているもので、電子計算機１０は外部メモリ１５から取込まれる暗号化プログラムをそのヘッダ等に付加された情報に基づいて暗号化プログラムであることを判断し、暗号部分の解読を開始する。

【００２４】前記外部メモリ１５から暗号化プログラムの暗号部分が電子計算機１０から取込まれると、その暗号部分は、内蔵ＲＯＭ１２に予め記憶されている暗号解読プログラムに従って解読されるもので、この暗号解読プログラムに従って解読されたプログラムは、内蔵キャッシュメモリ１３に書込まれる（ステップＳ３，Ｓ４）。

【００２５】ここで、前記内蔵ＲＯＭ１２の記憶内容は、外部バスには読出しできない構成とされるので、暗号解読プログラムのアルゴリズムが第３者に解析される恐れはない。

【００２６】そして、前記暗号化プログラムの暗号部分が解読され、内蔵キャッシュメモリ１３に書込まれると、この解読されたプログラムの記憶領域におけるデータページ等のキャッシュの機能を制御するための制御レジスタ１４に対して、キャッシュ機能の禁止を指示するフラグをセットし、解読されたプログラムの外部バスへの読出し禁止が図られる（ステップＳ５）。

【００２７】こうして、内蔵キャッシュメモリ１３のキャッシュ機能の禁止領域において書込まれた解読されたプログラムは、前記外部メモリ１５にロードされた暗号化プログラムの中のもともと暗号化されていない部分の非暗号部分のプログラムと組合され、ＣＰＵ１１に読出されて実行される（ステップＳ６，Ｓ７）。

【００２８】つまり、前記外部メモリ１５にロードされた暗号化プログラムのうち、その暗号部分のプログラムは、解読されて電子計算機１０の内蔵キャッシュメモリ１３の一部に常駐し、また、それ以外の非暗号部分のプログラムは、キャッシュメモリ１３の残りの部分を用いて通常のキャッシュ動作によって実行される。

【００２９】この後、前記暗号化プログラムの実行が不要になった場合には、内蔵キャッシュメモリ１３に書込まれた暗号解読後のプログラムが消去されると共に、その記憶領域に対応させて、制御レジスタ１４におけるキャッシュ機能禁止のフラグが解除される。

【００３０】したがって、前記第１実施例の構成の暗号化プログラム演算装置を搭載した電子計算機１０によれば、外部メモリ１５にロードされた暗号化プログラムの暗号部分を電子計算機１０に取込んで、外部バスに読出し不可能な内蔵ＲＯＭ１２に予め記憶されている暗号解読プログラム従って解読し、内蔵キャッシュメモリ１３に記憶させると共に、この内蔵キャッシュメモリ１３の

前記解読されたプログラムの記憶領域に対応させて、制御レジスタ１４にキャッシュ機能の禁止フラグをセットすることで該解読されたプログラムの外部バスへの読出しも禁止し、この解読後プログラムと前記外部メモリ１５に記憶されている非暗号化部分のプログラムと組合されてＣＰＵ１１により実行されるので、暗号解読用のプログラム自体がコピーされて解読されてしまったり、解読された後の暗号プログラムがコピーされて利用される等の問題を、電子計算機１０の簡単な構成変更により解消することができる。

【００３１】これにより、暗号化プログラムを特定の電子計算機にて専用の暗号解読プログラムにより解読して利用する場合に、第３者にその解読プログラムや解読後プログラムが読出されることのない信頼性の高い暗号化プログラム演算装置を提供できる。

【００３２】なお、前記実施例では、解読されたプログラムを内蔵キャッシュメモリ１３に書込んだ際に、その書込み領域におけるキャッシュの機能を制御レジスタ１４により禁止して、外部バスへの読出し禁止を図っているが、例えば図３及び図４における第２実施例の暗号化プログラム演算装置で示すように、前記内蔵キャッシュメモリ１３に対する解読されたプログラムの書込みと同時にその読出し禁止フラグを付加する命令をＣＰＵ２１のシステムプログラムに持たせる構成とすれば、前記キャッシュ機能の禁止／禁止解除を行なう制御レジスタが不要になるので、解読されたプログラムの読出しがより困難な構成とすることができる。

【００３３】図３は本発明の第２実施例に係わる暗号化プログラム演算装置を搭載した電子計算機２０の構成を示すブロック図である。この電子計算機２０は、ＣＰＵ２１を備えている。

【００３４】前記ＣＰＵ２１は、内蔵ＲＯＭ１２に予め記憶されているプログラムに従って回路各部の動作制御を実行するもので、このＣＰＵ１１には、データ及び制御バスを介して前記内蔵ＲＯＭ１２の他、内蔵キャッシュメモリ１３が接続される。

【００３５】前記内蔵キャッシュメモリ１３は、データ書込みに伴なうＣＰＵ２１からの強制書込み命令により、当該データ書込み領域におけるキャッシュ機能（データの追出し，書込み機能）の禁止が制御される構成とする。

【００３６】また、前記ＣＰＵ２１は、外部メモリ１５に記憶されているプログラムの読込みを行なった場合には、その読込んだプログラムに従って制御動作を実行する。ここで、前記内蔵ＲＯＭ１２には、予め暗号解読プログラムが記憶され、また、この内蔵ＲＯＭ１２の記憶内容は、外部バスには読出しできない構成とする。

【００３７】なお、前記外部メモリ１５に記憶されるプログラムデータは、例えば公共の有線放送や無線放送、あるいはメモリカード等の利用により得られるデータであってもよい。

【００３８】そして、前記外部メモリ１５から読込まれたプログラムデータが、暗号解読の不要な通常のプログラムデータである場合には、ＣＰＵ１１は内蔵キャッシュメモリ１３のキャッシュ機能を通常に使用してその読込みプログラムデータにそのまま従った制御動作を実行する。

【００３９】次に、前記第２実施例の構成による暗号化プログラム演算装置を搭載した電子計算機２０における暗号化プログラムの実行動作について説明する。図４は前記第２実施例に係わる暗号化プログラム演算装置を搭載した電子計算機２０における暗号化プログラムの実行処理を示すフローチャートである。

【００４０】すなわち、暗号解読が必要な暗号化プログラムが外部メモリ１５にロードされると、この暗号化プログラムは電子計算機２０に取込まれその暗号部分の解読が開始される（ステップＡ１，Ａ２）。

【００４１】前記暗号化プログラムは、そのプログラム全体の一部あるいは全てがコマンド，データの区別なく暗号化されており、ヘッダ等において暗号化プログラムであることの情報が付加されているもので、電子計算機２０は外部メモリ１５から取込まれる暗号化プログラムをそのヘッダ等に付加された情報に基づいて暗号化プログラムであることを判断し、暗号部分の解読を開始する。

【００４２】前記外部メモリ１５から暗号化プログラムの暗号部分が電子計算機２０から取込まれると、その暗号部分は、内蔵ＲＯＭ１２に予め記憶されている暗号解読プログラムに従って解読されるもので、この暗号解読プログラムに従って解読されたプログラムは、内蔵キャッシュメモリ１３に書込まれる（ステップＡ３，Ａ４）。

【００４３】この場合、前記解読されたプログラムの内蔵キャッシュメモリ１３への書込み処理は、ＣＰＵ２１からの強制書込み命令により行なわれ、該キャッシュメモリ１３におけるプログラム書込み領域には、その書込みと同時に読出し禁止フラグがセットされ、外部バスへの読出しが禁止される。

【００４４】一方、前記内蔵ＲＯＭ１２の記憶内容は、外部バスには読出しできない構成とされるので、暗号解読プログラムのアルゴリズムが第３者に解析される恐れはない。

【００４５】こうして、内蔵キャッシュメモリ１３に読出し禁止フラグが付加されて書込まれた解読されたプログラムは、前記外部メモリ１５にロードされた暗号化プログラムの中のもともと暗号化されていない部分の非暗号部分のプログラムと組合され、ＣＰＵ１１に読出されて実行される（ステップＡ５，Ａ６）。

【００４６】つまり、前記外部メモリ１５にロードされた暗号化プログラムのうち、その暗号部分のプログラム

は、電子計算機２０の内蔵キャッシュメモリ１３に書込まれた暗号解読後のプログラムに従って実行され、また、それ以外の非暗号部分のプログラムは、そのまま読出されて実行される。

【００４７】この後、前記暗号化プログラムの実行が不要になった場合には、内蔵キャッシュメモリ１３にセットされている読出し禁止フラグが解除され、そこに書込まれている暗号解読後のプログラムが消去される。

【００４８】したがって、前記第２実施例の構成の暗号化プログラム演算装置を搭載した電子計算機２０によれば、外部メモリ１５にロードされた暗号化プログラムの暗号部分を電子計算機２０に取込んで、外部バスに読出し不可能な内蔵ＲＯＭ１２に予め記憶されている暗号解読プログラム従って解読し、内蔵キャッシュメモリ１３にＣＰＵ２１からの強制書込み命令により書込むと共に、この内蔵キャッシュメモリ１３に対する前記命令によりそのプログラム書込み領域に対応させて読出し禁止フラグをセットし、この解読後プログラムと前記外部メモリ１５に記憶されている非暗号化部分のプログラムと組合されてＣＰＵ２１により実行されるので、暗号解読用のプログラム自体がコピーされて解読されてしまったり、解読された後の暗号プログラムがコピーされて利用される等の問題を、電子計算機２０の簡単な構成変更により解消することができる。

【００４９】よって、前記第１実施例の暗号化プログラム演算装置と比較して、キャッシュ機能の禁止／禁止解除を行なう制御レジスタが不要になるので、解読されたプログラムの読出しがより困難な構成とすることができる。

【００５０】

【発明の効果】以上のように、本発明の請求項１に係わる暗号化プログラム演算装置によれば、第１のメモリに記憶された暗号解読プログラムにより解読された暗号プログラムが第２のメモリに記憶され、この第２のメモリに記憶された解読された暗号プログラムの外部への読出しが禁止されるようになる。

【００５１】また、本発明の請求項２係わる暗号化プログラム演算装置によれば、請求項１に係わる暗号化プログラム演算装置にあって、暗号プログラムの実行モードを記憶する制御レジスタの内容に従って第２のメモリに記憶された解読された暗号プログラムの外部への読出しが禁止されるようになる。

【００５２】また、本発明の請求項３に係わる暗号化プログラム演算装置によれば、請求項１に係わる暗号化プログラム演算装置にあって、暗号解読プログラムにより解読された暗号プログラムが第２のメモリに記憶される際には、読出し禁止フラグが付けられて外部への読出しが禁止されるようになる。

【００５３】また、本発明の請求項４に係わる暗号化プログラム演算装置によれば、請求項２又は請求項３何れか１項に係わる暗号化プログラム演算装置にあって、第２のメモリがキャッシュメモリとされ、暗号プログラムの実行時には、解読された暗号プログラムの記憶領域の追出し，書込みが禁止されるようになる。よって、暗号プログラムがコピーされて利用されるのを防止することが可能になる暗号化プログラム演算装置を提供できる。

【図面の簡単な説明】

【図１】本発明の第１実施例に係わる暗号化プログラム演算装置を搭載した電子計算機の構成を示すブロック図。

【図２】前記第１実施例に係わる暗号化プログラム演算装置を搭載した電子計算機における暗号化プログラムの実行処理を示すフローチャート。

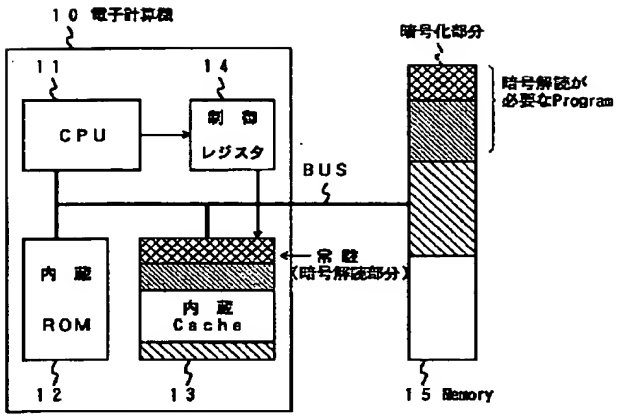
【図３】本発明の第２実施例に係わる暗号化プログラム演算装置を搭載した電子計算機の構成を示すブロック図。

【図４】前記第２実施例に係わる暗号化プログラム演算装置を搭載した電子計算機における暗号化プログラムの実行処理を示すフローチャート。

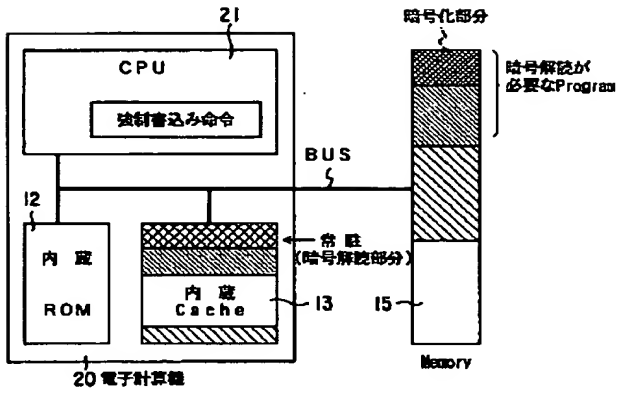
【符号の説明】

１０、２０…電子計算機、１１、２１…ＣＰＵ、１２…内蔵ＲＯＭ、１３…内蔵キャッシュメモリ、１４…制御レジスタ、１５…外部メモリ。

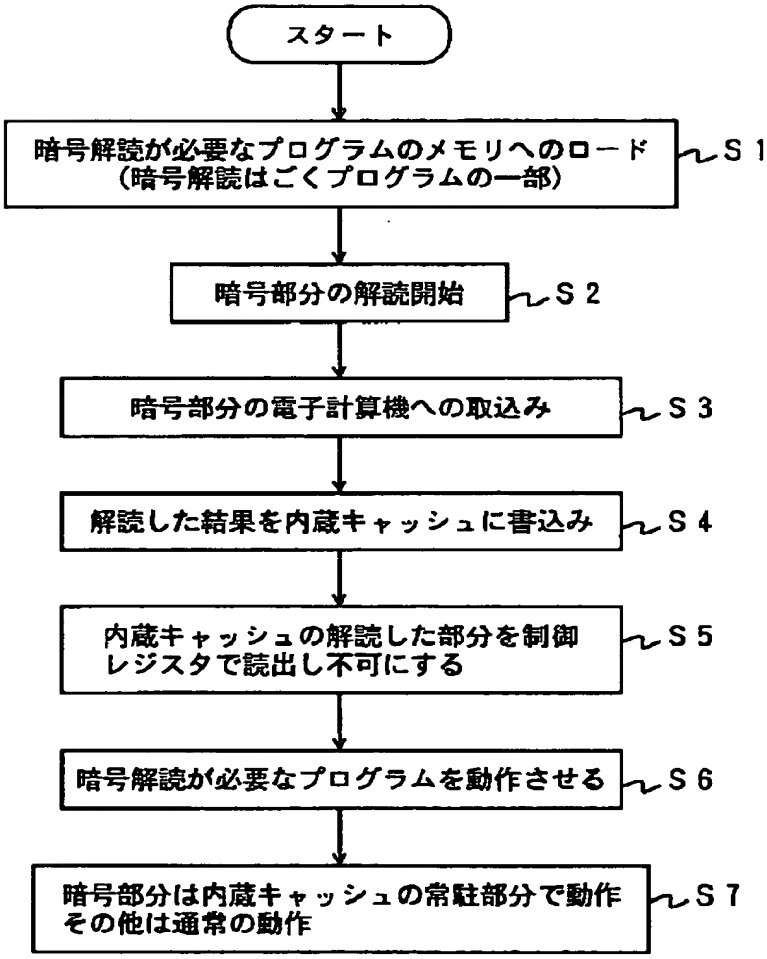
【図１】


１０ 電子計算機
１１
１４
CPU
制 御
レジスタ
BUS
暗号化部分
暗号解読が
必要なProgram
内 蔵
ROM
内 蔵
Cache
常 駐
（暗号解読部分）
１２
１３
１５ Memory

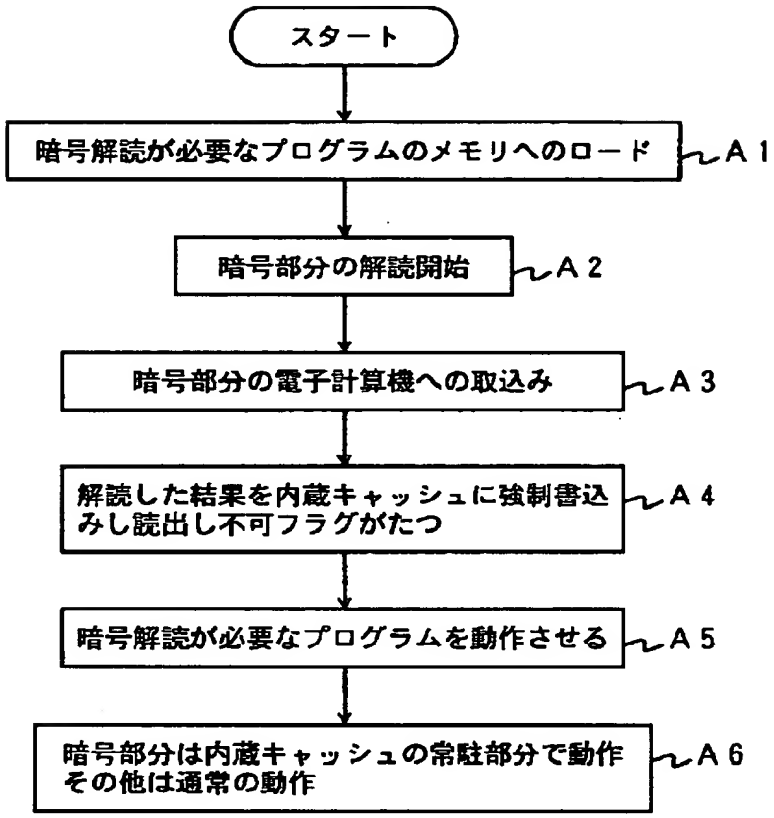
【図３】


２１
暗号化部分
CPU
強制書込み命令
暗号解読が
必要なProgram
BUS
１２
内 蔵
ROM
内 蔵
Cache
常 駐
（暗号解読部分）
１３
１５
Memory
２０ 電子計算機

【図２】


スタート
暗号解読が必要なプログラムのメモリへのロード
（暗号解読はごくプログラムの一部）
Ｓ１
暗号部分の解読開始
Ｓ２
暗号部分の電子計算機への取込み
Ｓ３
解読した結果を内蔵キャッシュに書込み
Ｓ４
内蔵キャッシュの解読した部分を制御
レジスタで読出し不可にする
Ｓ５
暗号解読が必要なプログラムを動作させる
Ｓ６
暗号部分は内蔵キャッシュの常駐部分で動作
その他は通常の動作
Ｓ７

【図４】



フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｌ　9/12				